PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-336624
(43)Date of publication of application : 18.12.1998

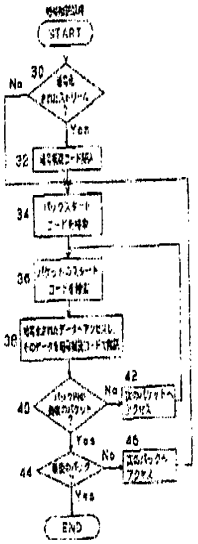
(51)Int.Cl. H04N 7/167

(21)Application number : 09-154396
(22)Date of filing : 28.05.1997

(71)Applicant : BROTHER IND LTD
(72)Inventor : TAKAHASHI HIDEAKI

(54) DEVICE AND METHOD FOR SCRAMBLING AND DESCRAMBLING MPEG STREAM DATA

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a device and a method capable of protecting MPEG stream data from unauthorized use without increasing the processing loads of a CPU for decoding the cipher of the MPEG stream data.
SOLUTION: At the time of judging that it is a ciphered stream in a step 30, a cipher decoding code stored in a RAM is read in the step 32, ciphered data are accessed in the steps 34-38 and the data are decoded by the cipher decoding code. In the step 38, the ciphered data of the total of 8 bytes that are the third byte of a packet start code, a stream ID, a PES(program elementary stream) packet length and a sequence header attached to packet data at the head of a GOP(group of pictures) are decoded. That is, since a data amount to be decoded is little, the processing loads of the CPU are reduced.



CLAIMS

[Claim(s)]
[Claim 1]Packet data.
A packet header attached in front of these packet data.

It is a scramble device of MPEG stream data provided with the above, A predetermined part of said packet header and a predetermined part of the beginning of packet data were enciphered, and it had a scramble means changed into a scramble state which cannot perform normal system decoding as it was.

[Claim 2]A packet start code said packet header indicates a start code of a packet to be, It has packet length data in which the length of stream ID information in which data which identifies a stream is shown, and a packet is shown, Packet data of a top packet among two or more packets which constitute each GOP, Have a sequence header at the head and said scramble means, A predetermined part of said packet start code, stream ID information, and packet strength data, A scramble device of the MPEG stream data according to claim 1 being that which is changed into a scramble state which enciphers said sequence header and cannot perform system decoding normal as it is.
[Claim 3]Packet data.
A packet header attached in front of these packet data.
It is a scrambling method of MPEG stream data provided with the above, a predetermined part of said packet header and a predetermined part of the beginning of packet data are enciphered, and it changes into a scramble state which cannot perform normal system decoding as it is.

[Claim 4]A packet start code said packet header indicates a start code of a packet to be, It has packet length data in which the length of stream ID information in which data which identifies a stream is shown, and a packet is shown, Packet data of a top packet among two or more packets which constitute each GOP, Have a sequence header at the head and A predetermined part of said packet start code, stream ID information, and packet strength data, A scrambling method of the MPEG stream data according to claim 3 changing into a scramble state which enciphers said sequence header and cannot perform system decoding normal as it is.
[Claim 5]Packet data in which the first predetermined part was enciphered.
A packet header as which it was given in front of these packet data, and a predetermined part was enciphered.
It had a descrambling means to have been a descrambling device of MPEG stream data provided with the above, and to restore to data which can system decode said each enciphered each predetermined part by a predetermined decryption means.

[Claim 6]While said packet header has packet length data in which the length of stream ID information in which a packet start code which shows a start code of a packet, and data which identifies a stream are shown, and a packet is shown, Inside of two or more packets which a predetermined part of these data is enciphered and constitute each GOP, A sequence header which packet data of a top packet have at the head is enciphered, and said descrambling means, A descrambling device of the MPEG stream data according to claim 5 characterized by being what restores said each enciphered predetermined part to data in which system decoding is possible by said predetermined decryption means.
[Claim 7]Packet data in which the first predetermined part was enciphered.
A packet header as which it was given in front of these packet data, and a predetermined part was enciphered.
It is the descrambling method of MPEG stream data provided with the above, and a predetermined decryption means restores to data which can system decode said enciphered each predetermined part.

[Claim 8]While said packet header has packet length data in which the length of stream ID information in which a packet start code which shows a start code of a packet, and data which

identifies a stream are shown, and a packet is shown, A predetermined field of these data is enciphered, and a sequence header which packet data of a top packet have at the head among two or more packets which constitute each GOP is enciphered, and by said predetermined decryption means. A descrambling method of the MPEG stream data according to claim 7 restoring said enciphered each predetermined part to data in which system decoding is possible.
[Claim 9]Packet data.
A packet header attached in front of these packet data.
It is the storage with which MPEG stream data provided with the above were memorized, a predetermined part of said packet header and a predetermined part of the beginning of packet data are enciphered, and it is in a scramble state which cannot perform normal system decoding as it is.

[Translation done.]

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention relates to the device and method for protecting the MPEG stream data coded based on the MPEG standard from an unauthorized use.
[0002]
[Description of the Prior Art]Recently, the product and service using MPEG art are spreading and, in many cases, copyright has generated a digital videodisc (DVD), digital video broadcast (DVB), etc. in the image work used with these products and services. Then, the problem how to protect the above-mentioned image work from a duplicate and use without an owner's of a copyright consent has surfaced.
[0003]
[Problem(s) to be Solved by the Invention]Although it is possible as the technique of solving the above-mentioned problem to encipher all the MPEG stream data, since the data of the MPEG stream data which make an animation contents is large scale, there is a problem that the processing load of CPU which performs encryption and decryption becomes large. Especially in the DVD player which reproduces a background video with a karaoke device etc. In order to be attached to one music and to carry out continuous reproduction of the background video [many (for example, eight pieces)], when the processing load of CPU for decryption becomes large, there is a problem that the processing speed which reads a background video data from DVD and is reproduced becomes slow.
[0004]Then, this invention aims at realization of the device and method of protecting MPEG stream data from an unauthorized use, without increasing the burden of the device which reproduces MPEG stream data.

[0005]
[Means for Solving the Problem]This invention in order to attain the above-mentioned purpose in the invention according to claim 1. It is a scramble device of MPEG stream data which make plurality of a packet which has packet data and the packet header attached in front of these packet data 1 GOP units, A predetermined part of said packet header and a predetermined part of the beginning of packet data are enciphered, and technical means of having had a scramble means changed into a scramble state which cannot perform normal system decoding are adopted as it is.
[0006]In the invention according to claim 2, in a scramble device of the MPEG stream data according to claim 1, said packet header, It has packet length data in which the length of stream ID information in which a packet start code which shows a start code of a packet, and data which identifies a stream are shown, and a packet is shown, Packet data of a top packet among two or more packets which constitute each GOP, Have a sequence header at the head and said scramble means, A predetermined part of said packet start code, stream ID information, and packet strength data and said sequence header are enciphered, and technical means that it is that which is changed into a scramble state which cannot perform normal system decoding are adopted as it is.
[0007]It is a scrambling method of MPEG stream data which make plurality of a packet which has packet data and the packet header attached in front of these packet data in the invention according to claim 3 1 GOP units, A predetermined part of said packet header and a predetermined part of the beginning of packet data are enciphered, and technical means of changing into a scramble state which cannot perform normal system decoding are adopted as it is.
[0008]In the invention according to claim 4, in a scrambling method of the MPEG stream data according to claim 3, said packet header, It has packet length data in which the length of stream ID information in which a packet start code which shows a start code of a packet, and data which identifies a stream are shown, and a packet is shown, Packet data of a top packet among two or more packets which constitute each GOP, Have a sequence header at the head and A predetermined part of said packet start code, stream ID information, and packet strength data, Said sequence header is enciphered and technical means of changing into a scramble state which cannot perform normal system decoding are adopted as it is.
[0009]Packet data in which the first predetermined part was enciphered in the invention according to claim 5, Are plurality of a packet which has the packet header as which it was given in front of these packet data, and a predetermined part was enciphered a descrambling device of MPEG stream data made into 1 GOP units, and by a predetermined decryption means. Technical means of having had a descrambling means to restore said each enciphered each predetermined part to data in which system decoding is possible are adopted.
[0010]In the invention according to claim 6, in a descrambling device of the MPEG stream data according to claim 5, said packet header, While having packet length data in which the length of stream ID information in which a packet start code which shows a start code of a packet, and data which identifies a stream are shown, and a packet is shown, Inside of two or more packets which a predetermined part of these data is enciphered and constitute each GOP, A sequence header which packet data of a top packet have at the head is enciphered, and technical means that it is what is restored to data which can system decode said each enciphered predetermined part are used for said descrambling means by said predetermined decryption means.
[0011]Packet data in which the first predetermined part was enciphered in the invention according to claim 7, Are plurality of a packet which has the packet header as which it was given in front of these packet data, and a predetermined part was enciphered the descrambling method of MPEG stream data made into 1 GOP units, and by a predetermined decryption means. Technical means of restoring said enciphered each predetermined part to data in which system decoding is possible are adopted.
[0012]In the invention according to claim 8, in a descrambling method of the MPEG stream data according to claim 7, said packet header, While having packet length data in which the length of

stream ID information in which a packet start code which shows a start code of a packet, and data which identifies a stream are shown, and a packet is shown, A predetermined field of these data is enciphered, and a sequence header which packet data of a top packet have at the head among two or more packets which constitute each GOP is enciphered, and by said predetermined decryption means. Technical means of restoring said enciphered each predetermined part to data in which system decoding is possible are adopted.

[0013]It is the storage with which MPEG stream data which make plurality of a packet which has packet data and the packet header attached in front of these packet data in the invention according to claim 9 1 GOP units were memorized, A predetermined part of said packet header and a predetermined part of the beginning of packet data are enciphered, and technical means of being in a scramble state which cannot perform normal system decoding are adopted as it is.

[0014]

[Function]According to claim 1 thru/or the invention according to claim 4, the above-mentioned scramble means enciphers the predetermined part of a packet header, and the predetermined part of the beginning of packet data, and changes them into the scramble state which cannot perform normal system decoding as it is. That is, in order to change into the scramble state which enciphers the predetermined part of a packet header, and the predetermined part of the beginning of packet data, and cannot perform system decoding normal as it is, If the side which reproduces MPEG stream data does not have a means to decode and descramble the predetermined part enciphered [above-mentioned], MPEG stream data are normally unreproducible. Thereby, MPEG stream data can be protected from unjust reproduction. The portions to encipher are only a predetermined part of a packet header, and a predetermined part of the beginning of packet data, and since they do not encipher all the MPEG stream data, they can reduce the processing load of CPU of both side reproduced side it supplies MPEG stream data.

[0015]And the technical means further materialized for protecting such MPEG stream data, So that it may indicate to claim 2 and claim 4 the above-mentioned packet header, It has packet length data in which the length of the stream ID information in which the packet start code which shows the start code of a packet, and the data which identifies a stream are shown, and a packet is shown, The packet data of a top packet among two or more packets which constitute each GOP, When it has a sequence header at the head, the above-mentioned scramble means The predetermined part of the above-mentioned packet start code, stream ID information, and packet strength data, The above-mentioned sequence header is enciphered and it is in changing into the scramble state which cannot perform normal system decoding as it is. That is, protection from the unauthorized use of MPEG stream data can be thickened by changing a packet header and the important data in packet data into a scramble state.

[0016]In claim 5 thru/or the invention according to claim 8, the above-mentioned descrambling means restores the first predetermined part as which the predetermined part and packet data in which the above-mentioned packet header was enciphered were enciphered by the predetermined decryption means to the data in which system decoding is possible. The MPEG stream data which have by this the predetermined part which changed into the scramble state by claim 1 thru/or the technical means according to claim 4 are renewable. The portions to encipher are only a predetermined part of a packet header, and a predetermined part of the beginning of packet data, and since all the MPEG stream data are not enciphered, they can reduce the processing load of CPU for decryption.

[0017]And the technical means further materialized for protecting such MPEG stream data are indicated to claim 6 and claim 8. That is, while the above-mentioned packet header has packet length data in which the length of the stream ID information in which the packet start code which shows the start code of a packet, and the data which identifies a stream are shown, and a packet is shown, The inside of two or more packets which the predetermined part of these data is enciphered and constitute each GOP, When the sequence header which the packet data of a top packet have at

the head is enciphered, the above-mentioned predetermined decryption means restores the above-mentioned descrambling means to the data which can system decode the predetermined part each enciphered [above-mentioned].

[0018]The predetermined part of the packet header of MPEG stream data and the predetermined part of the beginning of packet data the protection from the unauthorized use of the storage with which MPEG stream data were memorized is remembered to be like the invention according to claim 9 are enciphered.

It can attain as it is by being in the scramble state which cannot perform normal system decoding. That is, since the above-mentioned predetermined part is enciphered, if a means to decode the enciphered predetermined part is not used, the MPEG stream data memorized by the storage are unreproducible.

[0019]

[Embodiment of the Invention]Hereafter, one embodiment of the device for the scramble of the MPEG stream data of this invention and descrambling and a method is described with reference to figures. First, one embodiment of the scramble device (a scramble device is called hereafter) of the MPEG stream data of this invention and a method (a scrambling method is called hereafter) is described with reference to figures. Drawing 1 is an explanatory view showing the main composition of the scramble device of this embodiment with a block.

[0020]The scramble device 10 is equipped with the encode circuit 20 which inputs and PES-packet-izes the video signal of an analog inputted from the outside. The video encoder 21 which encodes the video signal of an analog inputted from the outside in this encode circuit 20, and is changed into a digital data line, It has PAKETTAIZA 22 which changes the video signal changed into the digital data line by this video encoder 21 into the MPEG stream data packet-ized according to the MPEG 2 standard.

[0021]This PAKETTAIZA 22 is equipped with CPU23 which processes enciphering predetermined data etc. while packet-izing the video signal outputted from the video encoder 21.

ROM24 the program for the decryption code for encryption, an enciphered program, and packet-izing, etc. were remembered to be, and RAM25 which store temporarily the decryption code read from this ROM24, a program, etc. are connected to this CPU23.

[0022]The MPEG stream data outputted from PAKETTAIZA 22 are inputted into the input interface 30, and the MPEG stream data outputted from this interface 30 are transmitted and stored temporarily via the bus 32 at the buffer memory 18. CPU12 which performs the output of encryption instructions to CPU23, the data output instructions to the buffer memory 18, etc. in the bus 32, ROM14 the program etc. which are executed by this CPU12 were remembered to be, and RAM16 which store temporarily the program etc. which were read from this ROM14 are connected.

[0023]The buffer memory 18 outputs the MPEG stream data memorized according to the data output instructions from CPU12 to the MPEG recorder 40 via the output interface 34. And MPEG data storage media, such as DVD(Digital Video Disc) 61A MPEG stream data were remembered to be, are created by this MPEG recorder 40.

[0024]Next, it is explained about the main composition of MPEG stream data with reference to drawing 2 shown with a block. MPEG stream data are constituted per pack.

The pack header is attached before the top pack.

Although a pack header is not illustrated, it comprises 2-bit data "10" for discriminating from pack start code and MPEG1 which shows the start of a pack, an SCR (System Clock Reference), stuffing length, stuffing bytes, etc. One pack comprises two or more PES(s) (Program Elementary Stream). One PES comprises packet data in which the video data of MPEG 2 is shown, and a packet header attached in front of these packet data.

[0025]The packet start code a packet header indicates the start of a packet to be, Stream ID for

discriminating from other MPEG stream data, the PES packet length who shows the length of a packet, The 2-bit data "10" for discriminating from MPEG1, PES control, It comprises PES header length who shows the length of a PES header, PTS (Presentation Time Stamp), DTS (Decording TimeStamp) which control the timing of data output, etc. PES control comprises a priority which shows the importance as data, copyright, CRC flag additional information which shows transmission bit error detection, and other information. moreover -- one GOP (Group Of Picture) is constituted by two or more packet data -- every -- in front of the packet data of the head of GOP, 4 bytes of sequence header for discriminating from other GOP(s) is attached. And ES (Elementary Stream) is constituted by two or more GOP(s). MPEG stream data have a management file which manages the data of a cipher decoding code, the maker of an image, a creation date, etc.

[0026]Next, the contents of processing of scrambling method slack CPU23 performed in order to encipher some MPEG stream data of the above-mentioned composition are explained with reference to drawing 3 and drawing 4. Drawing 3 is a flow chart which shows the contents of processing of CPU23. Drawing 4 (A) is an explanatory view showing the data to encipher, and the decryption code used in order to encipher and the enciphered data in hexadecimal numbers, respectively.
The figure (B) is an explanatory view showing the arithmetic contents for encryption.

[0027]A packet start code is 3 bytes of "00 00 01h" here, Stream ID is 1 byte of "E0h", and PES packet length is 2 bytes of "67 45 h", A sequence header presupposes that it is 4 bytes of "00 00 01B3", and explains to representation the case where a total of 8 bytes to the 4th byte of "B3" of "01h" to the 3rd byte of sequence header of a packet start code are enciphered. The decryption code used for encryption shall be 8 bytes of "89 AB CD EF F1 E1 D1 C1", as shown in drawing 4 (A).

[0028]First, CPU23 searches the pack start code of the head of a pack header (Step 10), and it searches the start code of a packet continuously (Step 12). Then, it accesses to the data of the specified packet, and it enciphers using a decryption code and the data is changed into the scramble state which cannot perform normal system decoding as it is (Step 14). That is, 3rd byte "01h" of a packet start code, "E0h" of stream ID, It accesses to "00 00 01 B3" of "45 67 h" and the sequence header of PES packet length, and these data is enciphered using an encryption code "89 AB CD EF F1 E1 D1 C1."

[0029]This encryption is performed by calculating the exclusive OR (EXOR) of the data to encipher and a decryption code, as shown in drawing 4 (B). As shown in drawing 4 (A), the data enciphered by this operation is set to "88 4B 88 88 F1 E1 D0 72", and is replaced with and used for data before this enciphered data is enciphered. That is, replace with 3rd byte "01h" of a packet start code, and "88", It replaces with "E0h" of stream ID, "4B" replaces with "45 67 h" of PES packet length, "8888" replaces with "00 00 01 B3" of a sequence header, and "F1 E1 D0 72" is used, respectively.

[0030]And CPU23 judges whether it is a packet of the last in a pack (Step 16), when it is not the last packet, it is accessed to (Step 16:No) and the following packet (Step 18), and it enciphers by performing the above-mentioned step 12 and Step 14. After completing encryption of the last packet (Step 16: Yes), CPU23, It progresses to Step 20 and judges whether the pack which enciphered is the last pack (Step 20), when it is not the last pack, it accesses to (Step 20:No) and the following pack (Step 22), and it enciphers to the packet in the pack (Step 12 - Step 18).

[0031]As mentioned above, since according to the scramble device and method of this embodiment only some data of MPEG stream data is enciphered and all the MPEG stream data are not enciphered, the processing load of CPU23 for encryption is mitigable. And since important data called the 3rd byte, stream ID, and the PES packet length of a packet start code can be enciphered and it can change into a scramble state, MPEG stream data can be thickly protected from an unauthorized use.

[0032]Next, one embodiment of the descrambling device (a descrambling device is called hereafter)

of the MPEG stream data of this invention and a method (the descrambling method is called hereafter) is described with reference to figures. First, the main composition of a descrambling device is explained with reference to drawing 5. Here, the DVD (Digital Video Disc) player provided with the descrambling device, especially the thing used for reproduction of a background video with a karaoke device are explained to representation as a descrambling device.

[0033]The DVD drive 61 to which the background video data (MPEG stream data) which shows a background video to DVD player 60 reads a background video data from DVD61A memorized by the file format, The DVD drive 62 to which a background video data similarly reads a background video data from DVD62A memorized by the file format is built in. The read head etc. which read the background video data which irradiated with the beam of light the motor for disk rotations which is not illustrated, the motor drive circuit, and the disc face, and was memorized by the disk are provided in both the DVD drives 61 and 62, respectively.

[0034]The buffer memory 65 which stores temporarily the background video data read from DVD61A and 62A, and the MPEG decoder circuit 66 which inputs the background video data outputted from the buffer memory 65, and is changed into the video signal of an analog are built in DVD player 60. DVD player 60 is equipped with the control circuit 63 which has CPU64 which performs processing for descrambling the scramble-ized data, etc. when reading a background video data from DVD61A and DVD62A.

ROM68 the program for the descrambling processing performed by CPU64, etc. were remembered to be by CPU64, RAM67 which stores temporarily the cipher decoding code etc. which were read from the management file memorized by the program read from this ROM68, DVD61A, and DVD62A is connected.

The DVD drives 61 and 62, the control circuit 63, CPU64, RAM67, and ROM68 are equivalent to the descrambling device of this invention.

[0035]Next, the contents of processing of descrambling method slack CPU64 performed in order to decode the data in which the MPEG stream data read from DVD61A and DVD62A were enciphered are explained with reference to the flow chart of drawing 6 in which it is shown. The MPEG stream data scramble-ized by the above-mentioned scramble device 10 and the method shall be memorized by DVD61A and DVD62A.

[0036]First, the MPEG stream data in which CPU64 was read from DVD61A and DVD62A, When it is MPEG stream data which whether they are MPEG stream data which have the enciphered data judges (Step 30), and have the enciphered data, a cipher decoding code is read from (Step 30:Yes) and RAM67 (Step 32).

[0037]Then, CPU64 searches the pack start code of the pack header of the pack which constitutes MPEG stream data (Step 34), and it searches the start code of a packet continuously (Step 36). Then, it accesses to the enciphered data (Step 38), the data is decoded using a cipher decoding code, and it changes into the descrambling state which can carry out system decoding normally (Step 38). That is, the 3rd byte of "88" as which the packet start code was enciphered, It accesses to "F1 E1 D0 72" of "8888" and the enciphered sequence header of "4B" of enciphered stream ID, and the enciphered PES packet length, These data is decoded using a cipher decoding code "89 AB CD EF F1E1 D1 C1."

[0038]This decipherment is performed by calculating the exclusive OR (EXOR) of the enciphered data and a cipher decoding code, as shown in drawing 4 (B). it being set to "01h E0h 45 67h00 00 01B3h", and being restored to data before being enciphered, and the data enciphered by this operation, as shown in drawing 4 (A). CPU64 judges whether it is a packet of the last in a pack (Step 40), when it is not the last packet, it is accessed to (Step 40:No) and the following packet (Step 42), it performs the above-mentioned step 36 and Step 38, and decodes a code. After completing encryption of the last packet (Step 40: Yes), CPU64, Progress to Step 44 and it is judged whether the pack which decoded is the last pack (Step 44), When it is not the last pack, it accesses to (Step 44:No) and the following pack (Step 46), and a code is decoded to the packet in the pack (Step 34 -

Step 42).
[0039]As mentioned above, according to the descrambling device and method of this embodiment, the MPEG stream data scramble-ized by the above-mentioned scramble device 10 and the method can be descrambled, and it can reproduce. And since there is little data volume which decodes a code, the processing load of CPU64 for decryption is mitigable. Although the above-mentioned embodiment explained the case where enciphered the 3rd byte, stream ID, PES packet length, and sequence header of a packet start code, and the they-enciphered data was decoded, the data enciphered and decoded is not limited to them.
[0040]By the way, the thing of specification which can perform multiangle reproduction which changes and displays the angle which looks at the image reproduced, and multi-story reproduction which reproduces two or more stories selectively is in DVD. The navigation pack of composition of that a block shows to drawing 7 is given to these DVDs for every image file. This navigation pack has managed the data for realizing the above-mentioned reproduction.
It comprises a pack header, a system header, a padding header, etc.

[0041]A system header comprises various data for realizing 4 bytes of system header start code, 2 bytes of header length, and the above-mentioned reproduction. Then, for example, DVD of the specification which has a navigation pack can be protected from an unauthorized use by enciphering the 2nd byte of a system header start code, the 3rd byte, and a total of 4 bytes of header length using the above-mentioned scramble device and a method. Since the data volume enciphered also in this case is only 4 bytes, it can reduce the processing load of CPU of both side deciphered side it enciphers.
[0042]By the way, in each above-mentioned embodiment, the exclusive OR of encryption object data and a decryption code is calculated, Although the exclusive OR of the encryption method which replaces the calculated data with encryption object data, and uses it, and decryption object data and a cipher decoding code was calculated and how to restore by replacing with the data which had the calculated data enciphered was explained, It can replace with the above-mentioned exclusive OR, and methods, such as using logical sum (OR) and a logical product (AND), or changing for different data, can also be used. It enciphers that the enciphered data differs for every MPEG stream data, and decryption different, respectively can be performed. According to this, MPEG stream data can be protected from an unauthorized use still more thickly.
[0043]Although each above-mentioned embodiment explained the system which uses an MPEG data storage medium to representation, this invention is applicable to a VOD (Vide On Demand) server, digital broadcasting, the Internet, etc. Although the DVD player was explained to representation as a descrambling device, it is also applicable also to another CD-ROM player and MPEG data reproduction apparatus. Although each above-mentioned embodiment explained the case where a cipher decoding code was read from an MPEG data storage medium, and was provided to representation, The composition which forms a means (cipher decoding code reading means) to read the cipher decoding code which made the IC card etc. memorize a cipher decoding code, and was memorized by the IC card in an MPEG data reproduction apparatus can also be taken. If it is in the descrambling device with which the device which receives MPEG stream data via a communication line, and is reproduced was equipped, the composition which transmits a cipher decoding code to the above-mentioned device via the above-mentioned communication line can also be taken. ROM in a descrambling device, etc. can also memorize a cipher decoding code beforehand.
[0044]By the way, Step 10 to the step 22 performed by CPU23, It functions as the scramble device and method of MPEG stream data of this invention, and Step 46 functions from Step 30 performed by CPU64 as the descrambling device and method of MPEG stream data of this invention.
[0045]
[Effect of the Invention]According to this invention, the device and method of protecting MPEG stream data from an unauthorized use can be realized as mentioned above, without increasing the

burden of a device which reproduces MPEG stream data.

[Translation done.]

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]It is an explanatory view showing the main composition of the scramble device of this invention embodiment with a block.
[Drawing 2]It is an explanatory view showing the main composition of MPEG stream data with a block.
[Drawing 3]It is a flow chart which shows the contents of processing of CPU23.
[Drawing 4](A) is an explanatory view showing the data to encipher, and the decryption code used in order to encipher and the enciphered data in hexadecimal numbers, respectively, and (B) is an explanatory view showing the arithmetic contents for encryption.
[Drawing 5]It is an explanatory view showing the main composition of the DVD player provided with the descrambling device of this invention embodiment with a block.
[Drawing 6]It is an explanatory view showing the contents of processing of CPU64.
[Drawing 7]It is an explanatory view showing the composition of a navigation pack with a block.
[Description of Notations]
10 Scramble device
23,64 CPU
40 MPEG recorder
60 DVD player
61A,62A DVD

[Translation done.]

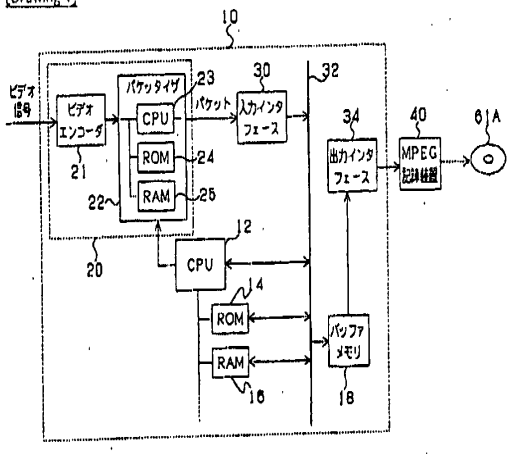
* NOTICES *

JPO and INPIT are not responsible for any
damages caused by the use of this translation.

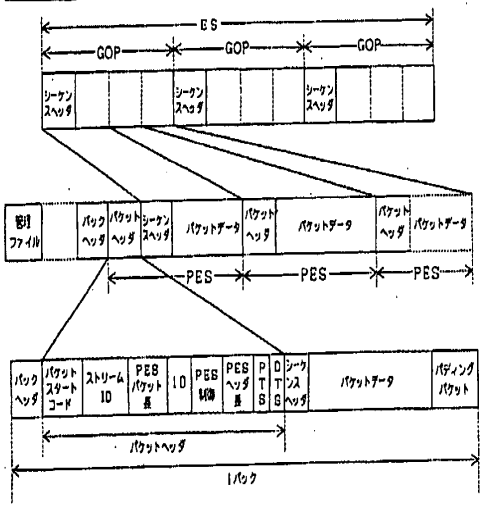
1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

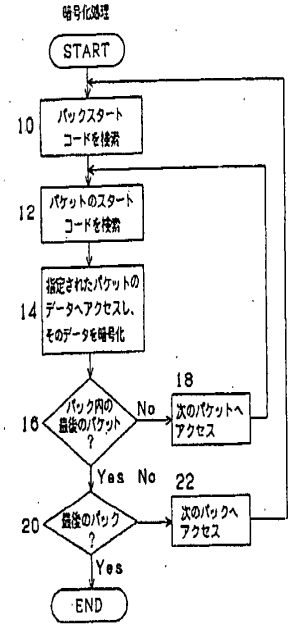
[Drawing 1]



[Drawing 2]



[Drawing 3]



[Drawing 4]

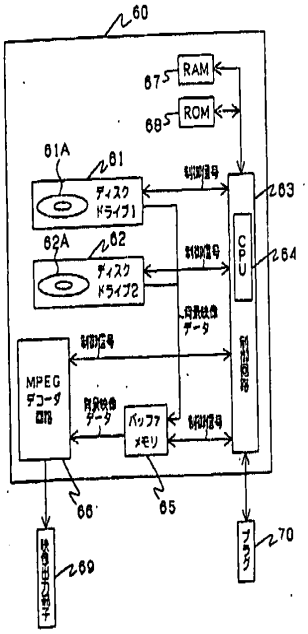
(A)

		パケットスタートコード3バイト目	ストリームID	PESパケット長	シーケンスヘッダ
A	暗号化するデータ	01h	E0h	45 67h	00 00 01 B3h
B	暗号(暗号解読)コード	89h	ABh	CD EFh	F1 E1 D1 C1h
C	暗号化されたデータ	88h	4Bh	88 88h	F1 E1 D0 72h

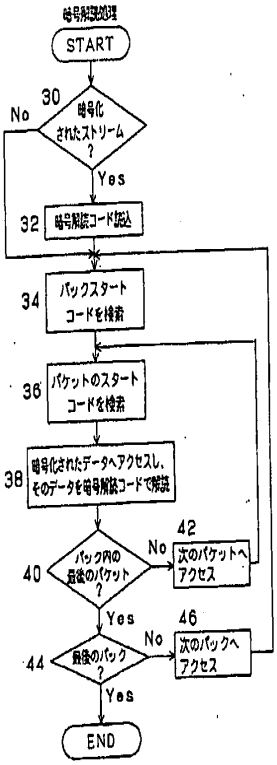
(B)

	パケットスタートコード3バイト目		ストリームID		PESパケット長				シーケンスヘッダ							
	0	1	E	0	4	5	6	7	0	0	0	0	0	1	B	3
A	0000	0001	1110	0000	0100	0101	0110	0111	0000	0000	0000	0000	0000	0001	1011	0011
	8	9	A	B	C	D	E	F	F	1	E	1	D	1	C	1
B	1000	1001	1010	1011	1100	1101	1110	1111	1111	0001	1110	0001	1101	0001	1100	0001
C	1000	1000	0100	1011	1000	1000	1000	1000	1111	0001	1110	0001	1101	0000	0111	0010
	8	8	4	B	8	8	8	8	F	1	E	1	D	0	7	2

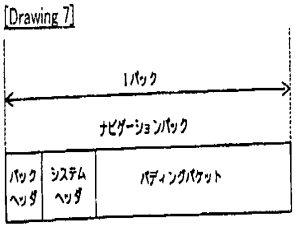
[Drawing 5]



[Drawing 6]



[Drawing 7]



[Translation done.]

D2

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平10－336624

(43)公開日　平成10年(1998)12月18日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｎ　7/167		Ｈ０４Ｎ　7/167	Ｚ

審査請求　未請求　請求項の数９　ＦＤ　（全 10 頁）

(21)出願番号　特願平9－154396

(22)出願日　平成９年(1997)５月28日

(71)出願人　000005267
ブラザー工業株式会社
愛知県名古屋市瑞穂区苗代町15番１号

(72)発明者　高橋　英彰
名古屋市瑞穂区苗代町15番１号　ブラザー工業株式会社内

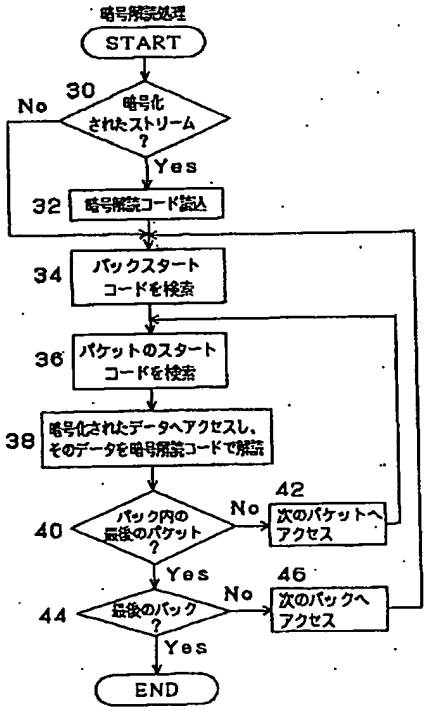
(74)代理人　弁理士　田下　明人　（外１名）

(54)【発明の名称】　ＭＰＥＧストリームデータのスクランブル、デスクランブルのための装置および方法

(57)【要約】

【課題】　ＭＰＥＧストリームデータの暗号を解読するためのＣＰＵの処理負荷を増大させることなくＭＰＥＧストリームデータを不正使用から保護できる装置および方法を実現する。

【解決手段】　ステップ３０で暗号化されたストリームと判定されると、ステップ３２でＲＡＭに記憶されている暗号解読コードを読込み、ステップ３４から３８で暗号化されたデータへアクセスし、そのデータを暗号解読コードで解読する。ステップ３８ではパケットスタートコードの３バイト目、ストリームＩＤ、ＰＥＳパケット長およびＧＯＰの先頭のパケットデータに付されたシーケンスヘッダの計８バイトの暗号化されたデータを解読する。つまり、解読するデータ量が少ないため、ＣＰＵの処理負荷を軽減できる。



【0001】
【発明の属する技術分野】この発明は、MPEG規格に基づいて符号化されたMPEGストリームデータを不正使用から保護するための装置および方法に関する。
【0002】
【従来の技術】最近、デジタルビデオディスク（DVD）やデジタルビデオ放送（DVB）など、MPEG技術を用いた製品やサービスが普及しつつあり、これらの製品やサービスで使用される映像作品には、多くの場合、著作権が発生している。そこで、上記映像作品を著作権者の許諾なき複製や使用から、いかに保護するかという問題が浮上している。
【0003】
【発明が解決しようとする課題】上記問題を解決する手法として、MPEGストリームデータの総てを暗号化することが考えられるが、動画をコンテンツとするMPEGストリームデータのデータは大容量であるため、暗号化および暗号解読を行うCPUの処理負荷が大きくなるという問題がある。特に、カラオケ装置などで背景映像を再生するDVDプレーヤでは、1曲に付き多く（たとえば、8個）の背景映像を連続再生するため、暗号解読のためのCPUの処理負荷が大きくなると、DVDから背景映像データを読出して再生する処理速度が遅くなるという問題がある。
【0004】そこで、本発明は、MPEGストリームデータを再生する装置の負担を増大させることなく、MPEGストリームデータを不正使用から保護できる装置および方法の実現を目的とする。
【0005】
【課題を解決するための手段】本発明は、上記目的を達成するため、請求項1に記載の発明では、バケットデータと、このバケットデータの前に付されたバケットヘッダとを有するバケットの複数を1GOP単位とするMPEGストリームデータのスクランブル装置であって、前記バケットヘッダの所定部分およびバケットデータの最初の所定部分を暗号化し、そのままでは正常なシステムデコードができないスクランブル状態にするスクランブル手段が備えられたという技術的手段を採用する。
【0006】請求項2に記載の発明では、請求項1に記載のMPEGストリームデータのスクランブル装置において、前記バケットヘッダは、バケットのスタートコードを示すバケットスタートコード、ストリームを識別するデータを示すストリームIDデータおよびバケットの長さを示すバケットレングスデータを有し、各GOPを構成する複数のバケットのうち、先頭のバケットのバケットデータは、その先頭にシーケンスヘッダを有し、前記スクランブル手段は、前記バケットスタートコード、ストリームIDデータおよびバケットストレングスデータの所定部分と、前記シーケンスヘッダとを暗号化し、そのままでは正常なシステムデコードができないスクランブル状態にするものであるという技術的手段を採用する。
【0007】請求項3に記載の発明では、バケットデータと、このバケットデータの前に付されたバケットヘッダとを有するバケットの複数を1GOP単位とするMPEGストリームデータのスクランブル方法であって、前記バケットヘッダの所定部分およびバケットデータの最初の所定部分を暗号化し、そのままでは正常なシステムデコードができないスクランブル状態にするという技術的手段を採用する。
【0008】請求項4に記載の発明では、請求項3に記載のMPEGストリームデータのスクランブル方法において、前記バケットヘッダは、バケットのスタートコードを示すバケットスタートコード、ストリームを識別するデータを示すストリームIDデータおよびバケットの長さを示すバケットレングスデータを有し、各GOPを構成する複数のバケットのうち、先頭のバケットのバケットデータは、その先頭にシーケンスヘッダを有し、前記バケットスタートコード、ストリームIDデータおよびバケットストレングスデータの所定部分と、前記シーケンスヘッダとを暗号化し、そのままでは正常なシステムデコードができないスクランブル状態にするという技術的手段を採用する。
【0009】請求項5に記載の発明では、最初の所定部分が暗号化されたバケットデータと、このバケットデータの前に付され、所定部分が暗号化されたバケットヘッダとを有するバケットの複数を1GOP単位とするMPEGストリームデータのデスクランブル装置であって、所定の暗号解読手段により、前記各暗号化された各所定部分をシステムデコード可能なデータに復元するデスクランブル手段が備えられたという技術的手段を採用する。
【0010】請求項6に記載の発明では、請求項5に記載のMPEGストリームデータのデスクランブル装置において、前記バケットヘッダは、バケットのスタートコードを示すバケットスタートコード、ストリームを識別するデータを示すストリームIDデータおよびバケットの長さを示すバケットレングスデータを有するとともに、それらデータの所定部分が暗号化されており、各GOPを構成する複数のバケットのうち、先頭のバケットのバケットデータが先頭に有するシーケンスヘッダが暗号化されており、前記デスクランブル手段は、前記所定の暗号解読手段により、前記暗号化された各所定部分をシステムデコード可能なデータに復元するものであるという技術的手段を採用する。
【0011】請求項7に記載の発明では、最初の所定部分が暗号化されたバケットデータと、このバケットデータの前に付され、所定部分が暗号化されたバケットヘッダとを有するバケットの複数を1GOP単位とするMPEGストリームデータのデスクランブル方法であって、

所定の暗号解読手段により、前記各暗号化された所定部分をシステムデコード可能なデータに復元するという技術的手段を採用する。

【0012】請求項8に記載の発明では、請求項7に記載のMPEGストリームデータのデスクランブル方法において、前記パケットヘッダは、パケットのスタートコードを示すパケットスタートコード、ストリームを識別するデータを示すストリームIDデータおよびパケットの長さを示すパケットレングスデータを有するとともに、それらデータの所定の領域が暗号化されており、各GOPを構成する複数のパケットのうち、先頭のパケットのパケットデータが先頭に有するシーケンスヘッダが暗号化されており、前記所定の暗号解読手段により、前記各暗号化された所定部分をシステムデコード可能なデータに復元するという技術的手段を採用する。

【0013】請求項9に記載の発明では、パケットデータと、このパケットデータの前に付されたパケットヘッダとを有するパケットの複数を1GOP単位とするMPEGストリームデータが記憶された記憶媒体であって、前記パケットヘッダの所定部分およびパケットデータの最初の所定部分が暗号化されており、そのままでは正常なシステムデコードができないスクランブル状態になっているという技術的手段を採用する。

【0014】

【作用】請求項1ないし請求項4に記載の発明によれば、上記スクランブル手段は、パケットヘッダの所定部分およびパケットデータの最初の所定部分を暗号化し、そのままでは正常なシステムデコードができないスクランブル状態にする。つまり、パケットヘッダの所定部分およびパケットデータの最初の所定部分を暗号化し、そのままでは正常なシステムデコードができないスクランブル状態にするため、MPEGストリームデータを再生する側が、上記暗号化された所定部分を解読してデスクランブルする手段を有さなければ、MPEGストリームデータを正常に再生することができない。これにより、MPEGストリームデータを不正な再生から保護できる。また、暗号化する部分は、パケットヘッダの所定部分およびパケットデータの最初の所定部分のみであり、MPEGストリームデータの総てを暗号化しないため、MPEGストリームデータを供給する側および再生する側双方のCPUの処理負荷を軽減することができる。

【0015】そして、そのようなMPEGストリームデータを保護するための、より一層具体化した技術的手段は、請求項2および請求項4に記載するように、上記パケットヘッダが、パケットのスタートコードを示すパケットスタートコード、ストリームを識別するデータを示すストリームIDデータおよびパケットの長さを示すパケットレングスデータを有し、各GOPを構成する複数のパケットのうち、先頭のパケットのパケットデータが、その先頭にシーケンスヘッダを有する場合に、上記スクランブル手段が、上記パケットスタートコード、ストリームIDデータおよびパケットストレングスデータの所定部分と、上記シーケンスヘッダとを暗号化し、そのままでは正常なシステムデコードができないスクランブル状態にすることにある。つまり、パケットヘッダおよびパケットデータの中の重要なデータをスクランブル状態にすることにより、MPEGストリームデータの不正使用からの保護を厚くすることができる。

【0016】また、請求項5ないし請求項8に記載の発明では、上記デスクランブル手段は、所定の暗号解読手段により、上記パケットヘッダの暗号化された所定部分およびパケットデータの暗号化された最初の所定部分をシステムデコード可能なデータに復元する。これにより、請求項1ないし請求項4に記載の技術的手段により、スクランブル状態になった所定部分を有するMPEGストリームデータを再生できる。また、暗号化する部分は、パケットヘッダの所定部分およびパケットデータの最初の所定部分のみであり、MPEGストリームデータの総てが暗号化されていないため、暗号解読のためのCPUの処理負荷を軽減することができる。

【0017】そして、そのようなMPEGストリームデータを保護するための、より一層具体化した技術的手段は、請求項6および請求項8に記載される。つまり、上記パケットヘッダが、パケットのスタートコードを示すパケットスタートコード、ストリームを識別するデータを示すストリームIDデータおよびパケットの長さを示すパケットレングスデータを有するとともに、それらデータの所定部分が暗号化されており、各GOPを構成する複数のパケットのうち、先頭のパケットのパケットデータが先頭に有するシーケンスヘッダが暗号化されている場合に、上記デスクランブル手段は、上記所定の暗号解読手段により、上記各暗号化された所定部分をシステムデコード可能なデータに復元する。

【0018】また、MPEGストリームデータが記憶された記憶媒体の不正使用からの保護は、請求項9に記載の発明のように、記憶されているMPEGストリームデータのパケットヘッダの所定部分およびパケットデータの最初の所定部分が暗号化されており、そのままでは正常なシステムデコードができないスクランブル状態になっていることにより達成できる。つまり、上記所定部分が暗号化されているため、その暗号化された所定部分を解読する手段を用いなければ、記憶媒体に記憶されたMPEGストリームデータを再生できない。

【0019】

【発明の実施の形態】以下、本発明のMPEGストリームデータのスクランブル、デスクランブルのための装置および方法の一実施形態について図を参照して説明する。まず、本発明のMPEGストリームデータのスクランブル装置（以下、スクランブル装置と称する）および方法（以下、スクランブル方法と称する）の一実施形態

について図を参照して説明する。図1は、本実施形態のスクランブル装置の主要構成をブロックで示す説明図である。

【0020】スクランブル装置10には、外部から入力されたアナログのビデオ信号を入力してPESパケット化するエンコード回路20が備えられている。このエンコード回路20には、外部から入力されたアナログのビデオ信号をエンコードしてデジタルデータ列に変換するビデオエンコーダ21と、このビデオエンコーダ21によりデジタルデータ列に変換されたビデオ信号をMPEG2規格にしたがってパケット化されたMPEGストリームデータに変換するパケッタイザ22とが備えられている。

【0021】このパケッタイザ22には、ビデオエンコーダ21から出力されたビデオ信号をパケット化するとともに、所定のデータを暗号化するなどの処理を行うCPU23が備えられており、このCPU23には、暗号化のための暗号コード、暗号化プログラムおよびパケット化のためのプログラムなどが記憶されたROM24と、このROM24から読出された暗号コードやプログラムなどを一時記憶するRAM25とが接続されている。

【0022】パケッタイザ22から出力されたMPEGストリームデータは、入力インターフェース30に入力され、このインターフェース30から出力されたMPEGストリームデータは、バス32を介してバッファメモリ18に転送され、一時記憶される。バス32には、CPU23への暗号化指令の出力、バッファメモリ18に対するデータ出力指令などを行うCPU12と、このCPU12により実行されるプログラムなどが記憶されたROM14と、このROM14から読出されたプログラムなどを一時記憶するRAM16とが接続されている。

【0023】バッファメモリ18は、CPU12からのデータ出力指令に応じて、記憶しているMPEGストリームデータを出力インターフェース34を介してMPEG記録装置40へ出力する。そして、このMPEG記録装置40により、MPEGストリームデータが記憶されたDVD(Digital Video Disc)61AなどのMPEGデータ記憶媒体が作成される。

【0024】次に、MPEGストリームデータの主要構成について、それをブロックで示す図2を参照して説明する。MPEGストリームデータは、バック単位で構成されており、先頭のバックの前には、バックヘッダが付されている。バックヘッダは、図示しないが、バックの開始を示すバックスタートコード、MPEG1と識別するための2ビットのデータ「10」、SCR（System Clock Reference）、スタッフィング長、スタッフィング・バイトなどから構成される。1つのバックは、複数のPES（Program Elementary Stream）から構成されており、1つのPESは、MPEG2のビデオデータを示すパケットデータと、このパケットデータの前に付されたパケットヘッダとから構成される。

【0025】パケットヘッダは、パケットの開始を示すパケットスタートコード、他のMPEGストリームデータと識別するためのストリームID、パケットの長さを示すPESパケット長、MPEG1と識別するための2ビットのデータ「10」、PES制御、PESヘッダの長さを示すPESヘッダ長、データ出力のタイミングを制御するPTS（Presentation Time Stamp）およびDTS（Decording TimeStamp）などから構成される。PES制御は、データとしての重要度を示すプライオリティ、著作権、伝送ビットエラー検出を示すCRCフラグ付加情報、およびその他の情報から構成される。また、複数のパケットデータにより1つのGOP（Group Of Picture）が構成されており、各GOPの先頭のパケットデータの前には、他のGOPと識別するための4バイトのシーケンスヘッダが付されている。そして、複数のGOPによりES（Elementary Stream）が構成される。さらに、MPEGストリームデータは、暗号解読コード、映像の作成者、作成年月日などのデータを管理する管理ファイルを有する。

【0026】次に、上記構成のMPEGストリームデータの一部を暗号化するために実行されるスクランブル方法たるCPU23の処理内容について図3および図4を参照して説明する。図3は、CPU23の処理内容を示すフローチャートである。図4（A）は、暗号化するデータと、暗号化するために用いられる暗号コードおよび暗号化されたデータをそれぞれ16進数で示す説明図であり、同図（B）は、暗号化のための演算内容を示す説明図である。

【0027】なお、ここでは、パケットスタートコードは「00 00 01h」の3バイトであり、ストリームIDは「E0h」の1バイトであり、PESパケット長は「45 67h」の2バイトであり、シーケンスヘッダは「00 00 01B3」の4バイトであるとし、パケットスタートコードの3バイト目の「01h」からシーケンスヘッダの4バイト目の「B3」までの計8バイトを暗号化する場合を代表に説明する。また、暗号化に用いる暗号コードは、図4（A）に示すように、「89 AB CD EF F1 E1 D1 C1」の8バイトとする。

【0028】まず、CPU23は、バックヘッダの先頭のバックスタートコードを検索し（ステップ10）、続いてパケットのスタートコードを検索する（ステップ12）。続いて、指定されたパケットのデータへアクセスし、そのデータを暗号コードを用いて暗号化し、そのままでは正常なシステムデコードができないスクランブル状態にする（ステップ14）。つまり、パケットスタートコードの3バイト目の「01h」、ストリームIDの「E0h」、PESパケット長の「45 67h」およ

びシーケンスヘッダの「００　００　０１　Ｂ３」へアクセスし、これらのデータを暗号化コード「８９　ＡＢ　ＣＤ　ＥＦ　Ｆ１　Ｅ１　Ｄ１　Ｃ１」を用いて暗号化する。

【００２９】この暗号化は、図４（Ｂ）に示すように、暗号化するデータおよび暗号コードの排他論理和（ＥＸＯＲ）を演算することにより行う。この演算により暗号化されたデータは、図４（Ａ）に示すように、「８８　４Ｂ　８８　８８　Ｆ１　Ｅ１　Ｄ０　７２」となり、この暗号化されたデータが暗号化される前のデータに代えて用いられる。つまり、パケットスタートコードの３バイト目の「０１ｈ」に代えて「８８」が、ストリームＩＤの「Ｅ０ｈ」に代えて「４Ｂ」が、ＰＥＳパケット長の「４５　６７ｈ」に代えて「８８　８８」が、シーケンスヘッダの「００　００　０１　Ｂ３」に代えて「Ｆ１　Ｅ１　Ｄ０　７２」がそれぞれ用いられる。

【００３０】そして、ＣＰＵ２３は、バック内の最後のパケットであるかを判定し（ステップ１６）、最後のパケットでない場合は（ステップ１６：Ｎｏ）、次のパケットへアクセスし（ステップ１８）、上記ステップ１２およびステップ１４を実行して暗号化を行う。ＣＰＵ２３は、最後のパケットの暗号化を終了すると（ステップ１６：Ｙｅｓ）、ステップ２０へ進み、暗号化を行ったバックが最後のバックか否かを判定し（ステップ２０）、最後のバックでない場合は（ステップ２０：Ｎｏ）、次のバックへアクセスし（ステップ２２）、そのバック内のパケットに対して暗号化を行う（ステップ１２～ステップ１８）。

【００３１】以上のように、本実施形態のスクランブル装置および方法によれば、ＭＰＥＧストリームデータの一部のデータのみを暗号化し、ＭＰＥＧストリームデータの総てを暗号化しないため、暗号化のためのＣＰＵ２３の処理負荷を軽減することができる。しかも、パケットスタートコードの３バイト目、ストリームＩＤおよびＰＥＳパケット長という重要なデータを暗号化してスクランブル状態にすることができるため、ＭＰＥＧストリームデータを不正使用から厚く保護できる。

【００３２】次に、本発明のＭＰＥＧストリームデータのデスクランブル装置（以下、デスクランブル装置と称する）および方法（以下、デスクランブル方法と称する）の一実施形態について図を参照して説明する。まず、デスクランブル装置の主要構成について図５を参照して説明する。なお、ここでは、デスクランブル装置として、デスクランブル装置を備えたＤＶＤ(Digital Video Disc)プレーヤ、特にカラオケ装置で背景映像の再生に用いるものを代表に説明する。

【００３３】ＤＶＤプレーヤ６０には、背景映像を示す背景映像データ（ＭＰＥＧストリームデータ）がファイル形式で記憶されたＤＶＤ６１Ａから背景映像データを読出すＤＶＤドライブ６１と、同じく背景映像データがファイル形式で記憶されたＤＶＤ６２Ａから背景映像データを読出すＤＶＤドライブ６２とが内蔵されている。両ＤＶＤドライブ６１、６２には、図示しないディスク回転用のモータ、モータ駆動回路、ディスク面に光線を照射してディスクに記憶された背景映像データを読取る読取ヘッドなどがそれぞれ設けられている。

【００３４】また、ＤＶＤプレーヤ６０には、ＤＶＤ６１Ａ、６２Ａから読出された背景映像データを一時記憶するバッファメモリ６５と、バッファメモリ６５から出力される背景映像データを入力してアナログの映像信号に変換するＭＰＥＧデコーダ回路６６とが内蔵されている。さらに、ＤＶＤプレーヤ６０には、ＤＶＤ６１Ａ、ＤＶＤ６２Ａから背景映像データを読出す際にスクランブル化されたデータをデスクランブルするための処理などを行うＣＰＵ６４を有する制御回路６３が備えられており、ＣＰＵ６４には、ＣＰＵ６４により実行されるデスクランブル処理のためのプログラムなどが記憶されたＲＯＭ６８と、このＲＯＭ６８から読出されたプログラム、ＤＶＤ６１Ａ、ＤＶＤ６２Ａに記憶されている管理ファイルから読出された暗号解読コードなどを一時記憶するＲＡＭ６７とが接続されている。なお、ＤＶＤドライブ６１，６２、制御回路６３、ＣＰＵ６４、ＲＡＭ６７およびＲＯＭ６８が、本発明のデスクランブル装置に相当する。

【００３５】次に、ＤＶＤ６１ＡおよびＤＶＤ６２Ａから読出されたＭＰＥＧストリームデータの暗号化されたデータを解読するために実行されるデスクランブル方法たるＣＰＵ６４の処理内容について、それを示す図６のフローチャートを参照して説明する。なお、ＤＶＤ６１ＡおよびＤＶＤ６２Ａには、上記スクランブル装置１０および方法によりスクランブル化されたＭＰＥＧストリームデータが記憶されているものとする。

【００３６】まず、ＣＰＵ６４は、ＤＶＤ６１ＡおよびＤＶＤ６２Ａから読出されたＭＰＥＧストリームデータが、暗号化されたデータを有するＭＰＥＧストリームデータであるかを判定し（ステップ３０）、暗号化されたデータを有するＭＰＥＧストリームデータである場合は（ステップ３０：Ｙｅｓ）、ＲＡＭ６７から暗号解読コードを読込む（ステップ３２）。

【００３７】続いて、ＣＰＵ６４は、ＭＰＥＧストリームデータを構成するバックのバックヘッダのバックスタートコードを検索し（ステップ３４）、続いてパケットのスタートコードを検索する（ステップ３６）。続いて、暗号化されたデータへアクセスし（ステップ３８）、そのデータを暗号解読コードを用いて解読し、正常にシステムデコードできるデスクランブル状態にする（ステップ３８）。つまり、パケットスタートコードの暗号化された３バイト目の「８８」、暗号化されたストリームＩＤの「４Ｂ」、暗号化されたＰＥＳパケット長の「８８８８」および暗号化されたシーケンスヘッダの

「F1 E1 D0 72」へアクセスし、これらのデータを暗号解読コード「89 AB CD EF F1 E1 D1 C1」を用いて解読する。

【0038】この解読は、図4（B）に示すように、暗号化されたデータおよび暗号解読コードの排他論理和（EXOR）を演算することにより行う。この演算により暗号化されたデータは、図4（A）に示すように、「01h E0h 45 67h00 00 01 B3h」となり、暗号化される前のデータに復元されるそして、CPU64は、バック内の最後のバケットであるかを判定し（ステップ40）、最後のバケットでない場合は（ステップ40：No）、次のバケットへアクセスし（ステップ42）、上記ステップ36およびステップ38を実行して暗号の解読を行う。CPU64は、最後のバケットの暗号化を終了すると（ステップ40：Yes）、ステップ44へ進み、解読を行ったバックが最後のバックか否かを判定し（ステップ44）、最後のバックでない場合は（ステップ44：No）、次のバックへアクセスし（ステップ46）、そのバック内のバケットに対して暗号の解読を行う（ステップ34～ステップ42）。

【0039】以上のように、本実施形態のデスクランブル装置および方法によれば、上記スクランブル装置10および方法によりスクランブル化されたMPEGストリームデータをデスクランブルして再生することができる。しかも、暗号を解読するデータ量が少ないため、暗号解読のためのCPU64の処理負荷を軽減することができる。なお、上記実施形態では、バケットスタートコードの3バイト目、ストリームID、PESバケット長およびシーケンスヘッダを暗号化し、それら暗号化されたデータを解読する場合を説明したが、暗号化および解読するデータは、それらに限定されるものではない。

【0040】ところで、DVDの中には、再生される映像を見る角度を変えて表示するマルチアングル再生や、複数のストーリーを選択的に再生するマルチストーリー再生を行うことができる仕様のものがある。これらのDVDには、各映像ファイルごとに、図7にブロックで示す構成のナビゲーションバックが付されている。このナビゲーションバックは、上記再生を実現するためのデータを管理しているものであり、バックヘッダ、システムヘッダおよびパディングヘッダなどから構成される。

【0041】システムヘッダは、4バイトのシステムヘッダスタートコード、2バイトのヘッダ長、上記再生を実現するための各種データから構成される。そこで、たとえば、システムヘッダスタートコードの2バイト目、3バイト目およびヘッダ長の計4バイトを上記スクランブル装置および方法を用いて暗号化することにより、ナビゲーションバックを有する仕様のDVDを不正使用から保護することができる。この場合も、暗号化するデータ量は、わずか4バイトであるため、暗号化する側および暗号解読する側双方のCPUの処理負荷を軽減できる。

【0042】ところで、上記各実施形態では、暗号化対象データと暗号コードとの排他論理和を演算し、その演算されたデータを暗号化対象データに代えて用いる暗号化方法、ならびに、暗号解読対象データと暗号解読コードとの排他論理和を演算し、その演算されたデータを暗号化されたデータに代えることにより復元する方法を説明したが、上記排他論理和に代えて論理和（OR）、論理積（AND）を用いたり、異なるデータと入れ替えるなどの方法を用いることもできる。また、暗号化されたデータがMPEGストリームデータごとに異なるように暗号化を行い、それぞれ異なる暗号解読を行うようにすることもできる。これによれば、MPEGストリームデータを不正使用からより一層厚く保護できる。

【0043】また、上記各実施形態では、MPEGデータ記憶媒体を用いるシステムを代表に説明したが、VOD（Vide On Demand）サーバー、デジタル放送、インターネットなどにも本発明を適用することができる。さらに、デスクランブル装置としてDVDプレーヤを代表に説明したが、CD－ROMプレーヤその他のMPEGデータ再生装置にも適用することもできる。また、上記各実施形態では、暗号解読コードがMPEGデータ記憶媒体から読出されて提供される場合を代表に説明したが、暗号解読コードをICカードなどに記憶させ、そのICカードに記憶された暗号解読コードを読取る手段（暗号解読コード読取手段）をMPEGデータ再生装置に設ける構成を採ることもできる。さらに、MPEGストリームデータを通信回線を介して受信し再生する装置に備えられたデスクランブル装置にあっては、暗号解読コードを上記通信回線を介して上記装置へ送信する構成を採ることもできる。また、暗号解読コードをデスクランブル装置内のROMなどに予め記憶されておくこともできる。

【0044】ところで、CPU23により実行されるステップ10からステップ22が、本発明のMPEGストリームデータのスクランブル装置および方法として機能し、CPU64により実行されるステップ30からステップ46が、本発明のMPEGストリームデータのデスクランブル装置および方法として機能する。

【0045】

【発明の効果】以上のように本発明によれば、MPEGストリームデータを再生する装置の負担を増大させることなく、MPEGストリームデータを不正使用から保護できる装置および方法を実現することができる。

【図面の簡単な説明】

【図1】本発明実施形態のスクランブル装置の主要構成をブロックで示す説明図である。

【図2】MPEGストリームデータの主要構成をブロックで示す説明図である。

【図３】ＣＰＵ２３の処理内容を示すフローチャートである。

【図４】（Ａ）は、暗号化するデータと、暗号化するために用いられる暗号コードおよび暗号化されたデータをそれぞれ１６進数で示す説明図であり、（Ｂ）は、暗号化のための演算内容を示す説明図である。

【図５】本発明実施形態のデスクランブル装置を備えたＤＶＤプレーヤの主要構成をブロックで示す説明図である。

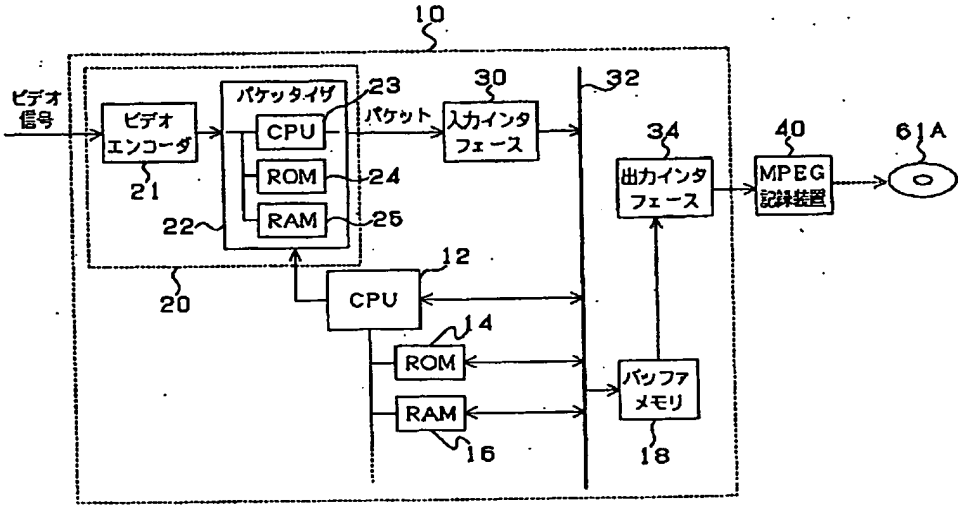
＊【図６】ＣＰＵ６４の処理内容を示す説明図である。

【図７】ナビゲーションバックの構成をブロックで示す説明図である。

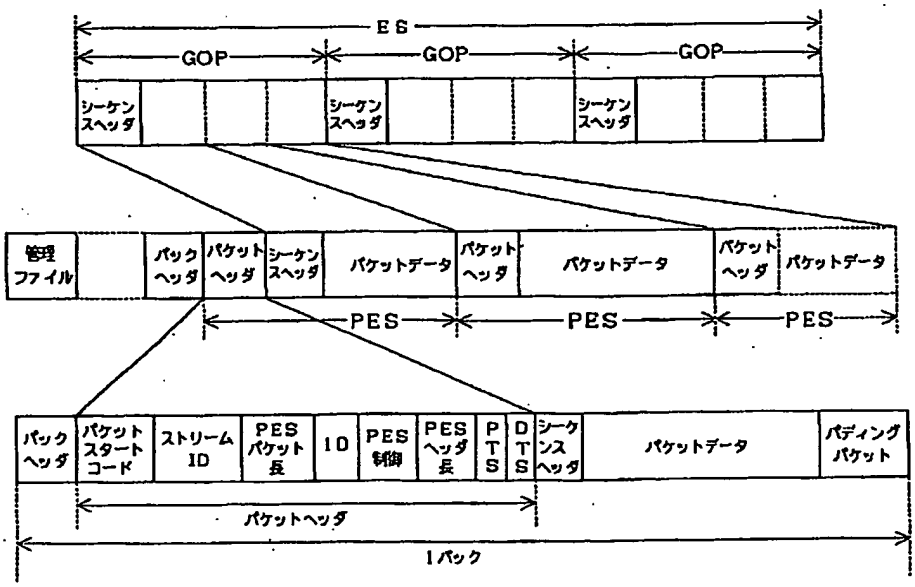
【符号の説明】

１０	スクランブル装置
２３，６４	ＣＰＵ
４０	ＭＰＥＧ記録装置
６０	ＤＶＤプレーヤ
＊　６１Ａ，６２Ａ	ＤＶＤ

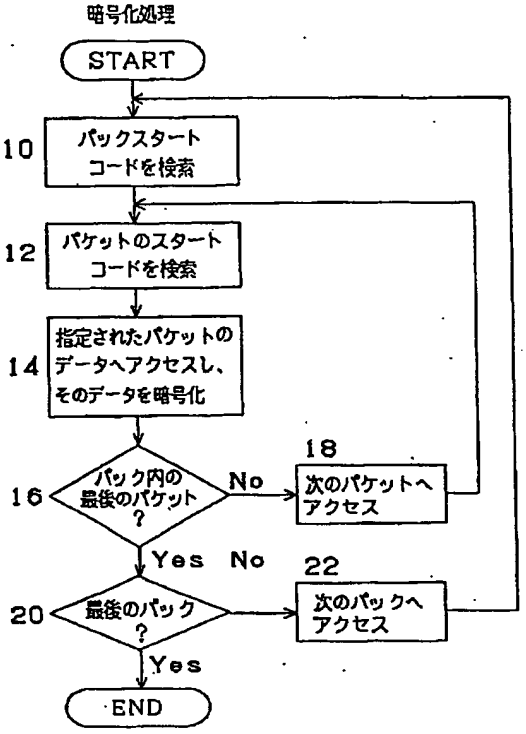
【図１】



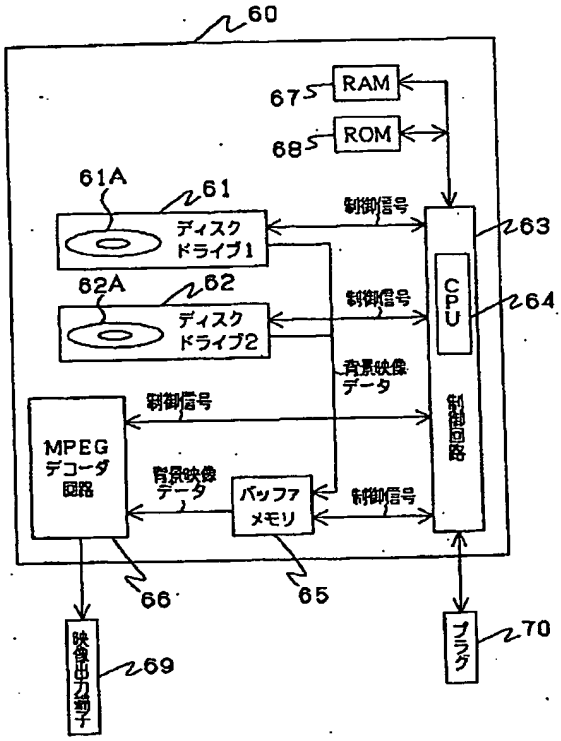
【図２】



【図3】



【図5】



【図4】

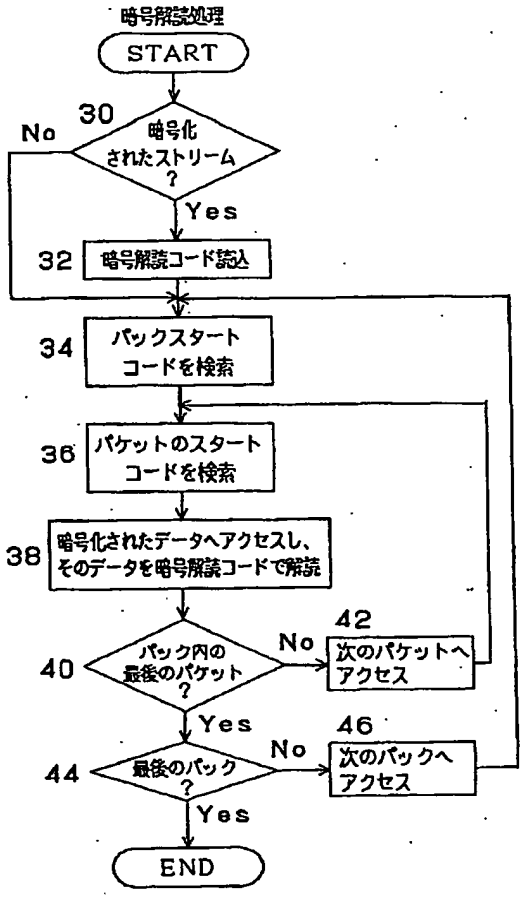
(A)

		パケットスタートコードの3バイト目	ストリームID	PES パケット長	シーケンスヘッダ
A	暗号化するデータ	01h	E0h	45 67h	00 00 01 B3h
B	暗号(暗号解読)コード	89h	ABh	CD EFh	F1 E1 D1 C1h
C	暗号化されたデータ	88h	4Bh	88 88h	F1 E1 D0 72h

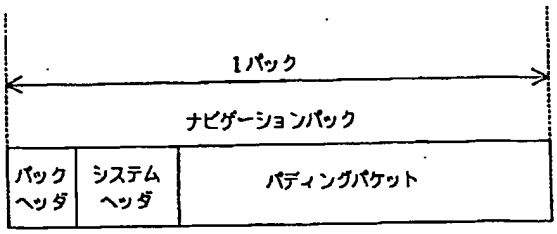
(B)

	パケットスタートコードの3バイト目		ストリームID		PES パケット長				シーケンスヘッダ							
A	0	1	E	0	4	5	6	7	0	0	0	0	0	1	B	3
	0000	0001	1110	0000	0100	0101	0110	0111	0000	0000	0000	0000	0000	0001	1011	0011
B	8	9	A	B	C	D	E	F	F	1	E	1	D	1	C	1
	1000	1001	1010	1011	1100	1101	1110	1111	1111	0001	1110	0001	1101	0001	1100	0001
C	1000	1000	0100	1011	1000	1000	1000	1000	1111	0001	1110	0001	1101	0000	0111	0010
	8	8	4	B	8	8	8	8	F	1	E	1	D	0	7	2

【図6】


暗号解読処理
START
30
暗号化されたストリーム？
No
Yes
32
暗号解読コード読込
34
パックスタートコードを検索
36
パケットのスタートコードを検索
38
暗号化されたデータへアクセスし、そのデータを暗号解読コードで解読
40
パック内の最後のパケット？
No
42
次のパケットへアクセス
Yes
44
最後のパック？
No
46
次のパックへアクセス
Yes
END

【図7】


1パック
ナビゲーションパック
パックヘッダ
システムヘッダ
パディングパケット